CLAIMS

WHAT IS CLAIMED IS:

1. A method of secure information distribution between nodes, the method comprising:

performing a handshake process with an adjacent node to determine membership in a secure group; and

distributing secure information to the adjacent node, if the adjacent node is a member of the secure group.

2. The method of claim 1, further comprising:

prior to providing the secure information to the adjacent node, performing the handshake process with another adjacent node.

3. The method of claim 1, further comprising:

establishing an encryption key with the adjacent node.

4. The method of claim 3, wherein the encryption key comprises a public key.

5. The method of claim 3, wherein the encryption key comprises a symmetric key.

6. The method of claim 3, wherein the secure information is distributed along with an encryption key.

7. The method of claim 1, wherein the action of performing the handshaking process comprises:

using a one way function f(x) to determine if the adjacent node is a member of the secure group.

8. The method of claim 7, wherein the one way function f(x) is a secure hash function.

9. The method of claim 1, wherein the action of performing the handshaking process comprises:

providing, by a first node, a component value A1 for a one way function f(x);

providing, by the adjacent node, a component value B1 as a challenge to the first node; and

applying the component values A1 and B1, and a key value SGK to the one way function f(x) to generate a value y.

10. The method of claim 9, wherein the one way function f(x) is a secure hash function.

11. The method of claim 1, wherein the secure information comprises a password.

12. The method of claim 1, wherein the secure information comprises a key for secure communication.

13. The method of claim 1, further comprising:

distributing secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

14. The method of claim 1, wherein the action of performing the handshake process comprises:

performing the handshake process with the adjacent node once for every fixed time amount T.

15. The method of claim 1, further comprising:

after detecting the presence of another node that is not in an adjacency set, attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0).

16. The method of claim 1, further comprising:

determining an age of the secure information so that each node in the secure group will store a latest version of the secure information.

17. The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a sequence number of the secure information to determine the age of the secure information.

18. The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a date of modification of the secure information to determine the age of the secure information.

19. The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking an elapsed time since a previous modification of the secure information to determine the age of the secure information.

20. The method of claim 1, further comprising:

resolving an ambiguity between a received updated secure information and currently stored secure information

by selecting the secure information with a larger data value.

21. The method of claim 1, further comprising:

increasing a security of the secure group by widening a secure group key (SGK) value which is known by each node in the secure group.

22. The method of claim 1, further comprising:

decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

23. The method of claim 1, further comprising:

allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.

24. The method of claim 1, further comprising:

preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between

handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.

25. An apparatus for secure information distribution between nodes, the apparatus comprising:

a node configured to performing a handshake process with an adjacent node to determine membership in a secure group, and distribute secure information to the adjacent node, if the adjacent node is a member of the secure group.

26. The apparatus of claim 25, wherein the node performs the handshake process with another adjacent node, prior to providing the secure information to the adjacent node.

27. The apparatus of claim 25, wherein the node is configured to establish an encryption key with the adjacent node.

28. The apparatus of claim 25, wherein the encryption key comprises a public key.

29. The apparatus of claim 25, wherein the encryption key comprises a symmetric key.

30. The apparatus of claim 27, wherein the secure information is distributed along with an encryption key.

31. The apparatus of claim 25, wherein the node is configured to use a one way function f(x) to determine if the adjacent node is a member of the secure group.

32. The apparatus of claim 31, wherein the one way function f(x) is a secure hash function.

33. The apparatus of claim 25, wherein the node is configured to provide a component value A1 for a one way function f(x), and wherein the adjacent node is configured to provide a component value B1 as a challenge to the first node; and wherein the node and adjacent node are configured to apply the component values A1 and B1, and a key value SGK to the one way function f(x) to generate a value y.

34. The apparatus of claim 33, wherein the one way function f(x) is a secure hash function.

35. The apparatus of claim 25, wherein the secure information comprises a password.

36. The apparatus of claim 25, wherein the secure information comprises a key for secure communication.

37. The apparatus of claim 25, wherein the node is configured to distribute the secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

38. The apparatus of claim 25, wherein the node is configured to perform the handshake process with the adjacent node once for every fixed time amount T.

39. The apparatus of claim 25, wherein the node is configured to attempt to handshake with another node if the node and the another node both have a handshake time remaining value of zero (0).

40. The apparatus of claim 25, wherein the node is configured to determine an age of the secure information so that each node in the secure group will store a latest version of the secure information.

41. The apparatus of claim 25, wherein the node is configured to check a sequence number of the secure information to determine the age of the secure information.

42. The apparatus of claim 25, wherein the node is configured to check a date of modification of the secure information to determine the age of the secure information.

43. The apparatus of claim 25, wherein the node is configured to check an elapsed time since a previous modification of the secure information to determine the age of the secure information.

44. The apparatus of claim 25, wherein the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value.

45. The apparatus of claim 25, wherein the node is configured to increase a security of the secure group by widening a secure group key (SGK) value which is known by each node in the secure group.

46. The apparatus of claim 25, wherein the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

47. The apparatus of claim 25, wherein the node is configured to allow for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.

48. The apparatus of claim 25, wherein the node is prevented from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.

49. An apparatus for secure information distribution between nodes, the apparatus comprising:

means for performing a handshake process with an adjacent node to determine membership in a secure group; and

means for distributing secure information to the adjacent node, if the adjacent node is a member of the secure group.

50. An article of manufacture, comprising:

a machine-readable medium having stored thereon instructions to:

perform a handshake process with an adjacent node to determine membership in a secure group; and

distribute secure information to the adjacent node, if the adjacent node is a member of the secure group.